

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): John B. Beavers

Assignee: Symantec Corporation

Title: SYSTEM AND METHOD FOR TRACKING AND FILTERING
ALERTS IN AN ENTERPRISE AND GENERATING ALERT
INDICATIONS FOR ANALYSIS

Serial No.: 10/080,574 Filed: February 25, 2002

Examiner: Nirav B. Patel Group Art 2135
Unit:

Docket No.: SYMC1023

Monterey, CA
May 31, 2006

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF

Dear Sir:

Pursuant to 37 CFR § 41.37(a)(1), Appellant files this
Appellant's Brief in support of the Notice of Appeal filed on
April 21, 2006.

06/06/2006 BABRAHA1 00000062 10080574

01 FC:1402

500.00 OP

Real Party in Interest

The assignee of the above-referenced patent application, Symantec Corporation, is the real party in interest.

RELATED APPEALS AND INTERFERENCES

No other prior and pending appeals, judicial proceedings or interferences are known to appellant, the appellant's legal representative, or Assignee, which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1-22 are pending in the application. Claims 1-4, 6-9, and 13-21 stand rejected. The rejection of Claims 1-4, 6-9, 13-21 is hereby appealed.

Claims 5, 10-12, and 22 stand objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claims and any intervening claims.

Status of Amendments

All amendments have been entered. Applicant notes that no Amendments were filed after the final Office Action dated December 21, 2005.

Summary of Claimed Subject Matter

With respect to both of the independent Claims 1 and 15, referring initially to Figure 3, Applicant's specification sets forth:

Figure 3 represents a typical assortment of device experts 11, 13, 15, 17, 19, and 21 **receiving a multitude of events 23 from enterprise devices (not shown)** such as a firewall, a server, a router, a modem, a wireless remote machine, etc. For example, the NT device expert 11 **may receive output from the server of a network**, whereas the firewall device expert 19 **may receive output from an internet or intranet firewall**. (Page 10, lines 17-23, emphasis added.)

Further, referring now to FIG. 4, Applicant's specification sets forth:

The **enterprise device is depicted by reference numeral 61 with an output 63**. ... The output 63 is translated at translation step 64 using translator files 65 to produce a common format event or message 67. ... **The translated event 67 is then compared in look up step 71 with entries or lines contained in the knowledge base table 69**. If a match occurs between the information in the translated event 67 and the table entries, additional knowledge is added to the translated event based on one or more matches. Then, a knowledge-containing translated event 73 is generated. The knowledge-containing translated or common format event 73 is then processed at 75 using one or more rule files 77. ... The rule processor can evaluate any number of things to determine whether or when the event stream 73 should be sent onward. ... (Page 11, line 19 to page 12, line 21, emphasis added.)

Device Expert Knowledge Base Table file. This file adds additional information such as threat codes and a user-friendly description of the event. (Page 15, line 12 to line 14, emphasis added.)

Grounds of rejection to be reviewed on appeal

1. Whether Claims 1-3, 6-8, 13-15, 17-20 and 21 are unpatentable under 35 U.S.C. § 103(a) over Houston et al. (2002/0019945) in view of Blakely-Fogel et al. (4,864,492)?

2. Whether Claims 4, 9 and 16 are unpatentable under 35 U.S.C. § 103(a) over Houston et al. in view of Blakely-Fogel et al., and further in view of Lim (2004/0250133)?

Argument

1. Claims 1-3, 6-8, 13-15, 17-20, and 21 are patentable over Houston et al. (2002/0019945) in view of Blakely-Fogel et al. (4,864,492).

As to Houston et al., the Examiner admits:

Houston doesn't teach that adding knowledge to the common format event using knowledge base table files to generate a knowledge-containing common format event. (Office Action dated July 27, 2005, page 3.)

Blakely-Fogel et al. does not cure this glaring deficiency in Houston et al. With regards to Blakely-Fogel et al., the Examiner states:

However, Blakely-Fogel teaches that adding knowledge (i.e. modifying or changing) to the common format event using knowledge base table files [Fig. 2] to generate a knowledge-containing common format event [Fig. 2 "Knowledge base table", Fig. 3 "change current data"]. (Office actions dated December 21, 2005 and July 27, 2005, page 3 in both, emphasis in original.)

In response, as set forth by the Applicant in the Amendment filed on October 20, 2005 at pages 10-14:

The Examiner's statement is respectfully traversed. Blakely-Fogel et al. teaches (1) the knowledge base comprises rules; (2) that if the user's input conforms to the rules then **the user's input becomes the current data in the current database**; and (3) that if the user's input does not conform to the rules, **the rule** the user needs to correct the error of the user's input **is displayed to the user**. Thus, the Examiner has failed to callout where Blakely-Fogel et al. teaches or suggests "adding knowledge (i.e. modifying or changing) **to the common format event** using knowledge base table files" as asserted by the Examiner, emphasis added.

Specifically, Blakely-Fogel et al. teaches (1) the knowledge base comprises rules:

The knowledge base 20 comprises rules 21 as shown in FIG. 2. The rules 21 contain expert knowledge about the network architecture and the network architecture adapters that are supported by the particular network architecture such as SNA. For example, a rule 21 may cover the type of information being supplied, such as whether the information supplied is a connection name. If it is a connection name, a rule will cover the allowable names a user may select. The rules may state which characters can comprise an allowable name. The rule might state that connection names can only comprise the letters between capital A and Capital Z, an asterisk *, and the dollar sign \$. (Col. 3, lines 63 to col. 4, line 7, emphasis added.)

Further, Blakely-Fogel et al. teaches (2) that if the user's input conforms to the rules then the user's input becomes the current data in the current database:

If the user's input conforms to the rules 21 of the network architecture, **then the user's input becomes the current data in the current data base 50** as it resides in I/O storage device 6 of 50 is referenced by field G of the reference pointers 23 of a knowledge rule 21. **The user's input replaces the data previously residing in the current data base 50.** (Col. 4, line 64 to col. 5, line 2, emphasis added.)

Finally, Blakely-Fogel et al. teaches (3) that if the user's input does not conform to the rules, the rule the user needs to correct the error of the user's input is displayed to the user:

If the user's input does not conform to the rules 21 of the network architecture, then the control 30 accesses the user interface 40 to display to the user the rule 21 the user needs to correct the error of the user's previous input, step 35. (Col. 5, lines 2 to line 6, emphasis added.)

Further, Applicant respectfully submits the Examiner has failed to make a prima facie obviousness rejection. Applicant notes that to make a prima facie obviousness rejection, the MPEP directs:

BASIC CONSIDERATIONS WHICH APPLY TO OBVIOUSNESS REJECTIONS

When applying 35 U.S.C. 103, the following tenets of patent law must be adhered to:

- (A) The claimed invention must be considered as a whole;
- (B) The references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination;
- (C) The references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention; and
- (D) Reasonable expectation of success is the standard with which obviousness is determined.

MPEP § 2141, Rev. 3, August 2005, p. 2100-125. It is noted that this directive stated "the following tenets . . . must be adhered to." Accordingly, failure to adhere to any one of these tenets means that a prima facie obviousness rejection has not been made.

The rejection fails to adhere to multiple of these tenets.

As demonstrated more completely below, the references have not been considered as a whole and the references do not suggest the desirability of making the combination. Pieces of the references have been extracted and selectively interpreted in view of Applicant's claims. Finally, there is no explanation of how the primary reference would work for its intended purpose following the modification.

Initially, Applicant notes that Blakely-Fogel et al. teaches:

This invention relates to ... **configuring a system in accordance with the protocol of the network architecture while providing the user with feedback indicative of problems associated with an invalid request to facilitate a valid user entry.** (Col. 1, lines 7-11, emphasis added.)

Thus, instead of considering Blakely-Fogel et al. as a whole as teaching configuring a system in accordance with the protocol of the network architecture while providing the user with feedback indicative of problems associated with an invalid request, the Examiner has extracted the term "knowledge base table" from Blakely-Fogel et al. and selectively interpreted the term in view of Applicant's claimed invention.

The support the Examiner provides for the Examiner's assertion the Blakely-Fogel et al. teaches "adding knowledge (i.e. modifying or changing) to the common format event using knowledge base table files" is "[Fig. 2 "Knowledge base table", Fig. 3 "change current data"]", emphasis in original.

However, as discussed above, the "knowledge base table" contains rules, the rules containing expert knowledge about the network architecture and the network architecture adapters. As also discussed above, the "change current data" occurs when the user's input becomes the current data in the current data base.

Thus considering Blakely-Fogel et al. as a whole, the Examiner has failed to callout how Blakely-Fogel et al. has anything to do with a common format event or security events in general.

For similar reasons, the Examiner has failed to callout where Houston et al., Blakely-Fogel et al., either alone or in combination, suggest the desirability or obviousness of the combination. Applicant respectfully submits the Examiner is using hindsight reconstruction to deprecate Applicant's claimed invention.

For at least the above reasons, Houston et al. in view of Blakely-Fogel et al. does not teach or suggest:

A method of producing at least one alert indication based on a number of events derived from an enterprise comprising:

providing a plurality of enterprise device outputs, at least a portion of the outputs having different formats, each output containing an event relating to an enterprise device;

translating each output into a common format event,
adding knowledge to the common format event using knowledge base table files to generate a knowledge-containing common format event; and
applying one or more rules from a set of rules to the knowledge-containing common format event to generate the alert indication,

as recited in Claim 1, emphasis added. Accordingly, Claim 1 is allowable Houston et al. in view of Blakely-Fogel et al. Claims 2-3, 6-8, 13-14, 21, which depend from Claim 1, are allowable for at least the same reasons as Claim 1.

For similar reasons, Houston et al. in view of Blakely-Fogel et al. does not teach or suggest:

A system for producing at least one alert indication based on a number of events derived from an enterprise comprising:

a plurality of enterprise devices, each device capable of producing an output;

a number of translation files, the translation files allowing the output to be translated into a common format event;

a number of knowledge base table files, matching of the common format event with one or more of the knowledge base table files **adding knowledge from the matched file** to generate a knowledge-containing common format event;

a number of rule files, the rule files governing generation of the alert indication,

as recited in Claim 15, emphasis added. Accordingly, Claim 15 is allowable over Houston et al. in view of Blakely-Fogel et al. Claims 17-20, which depend from Claim 15, are allowable for at least the same reasons as Claim 15.

In response to the Applicant's arguments, the Examiner substantially repeats the previous rejection:

Houston doesn't expressively mention that knowledge base table files which is utilized for adding knowledge to the common format event. However,

Blakely-Fogel teaches that adding knowledge (i.e. modifying or changing) to the common format event using knowledge base table files **[Fig. 2]** to generate a knowledge-containing common format event **[Fig. 2 "Knowledge base table", Fig. 3 "change current data" step 34, 36]**. Further, ... (Office Action dated December 21, 2005, pages 11-12, emphasis in original).

As this response to Applicant's arguments is substantially identical to the rejection traversed above, Applicant hereby traverses the Examiner's response for the reasons set forth above.

Further, in response to Applicant's argument that the Examiner has failed to establish a prima facie obviousness rejection, the Examiner states:

... Furthermore, the examiner recognizes that obviousness can only be established by combining or modifying the teaching of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivations to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. ... **In this case, the combination of Houston and Blakely-Fogel teach the claimed subject matter and the combination is sufficient.** (Office Action dated December 21, 2005, page 13, emphasis added.)

Applicant respectfully submit that the Examiner has simply stated an unsupported conclusion and thus has failed to rebut Applicant's argument that the Examiner has failed to establish a prima facie obviousness rejection. For these reasons, Applicant hereby traverses the Examiner's response for the reasons set forth above.

2. Claims 4, 9, and 16 are patentable over Houston et al. in view of Blakely-Fogel et al. and further in view of Lim (2004/0250133).

As set forth above, Claims 1, 15 are allowable over Houston et al. in view of Blakely-Fogel et al. Claims 4, 9 and Claim 16, which depend from Claim 1 and Claim 15, respectively,

are allowable over Houston et al. in view of Blakely-Fogel et al. for at least the same reasons as Claim 1 and Claim 15. The Examiner has failed to callout where Lim cures the previously described deficiencies in Houston et al. in view of Blakely-Fogel et al. Accordingly, Claims 4, 9 and 16 are allowable over Houston et al. in view of Blakely-Fogel et al. and further in view of Lim.

Claims appendix

1. (Original) A method of producing at least one alert indication based on a number of events derived from an enterprise comprising:

providing a plurality of enterprise device outputs, at least a portion of the outputs having different formats, each output containing an event relating to an enterprise device;

translating each output into a common format event,

adding knowledge to the common format event using knowledge base table files to generate a knowledge-containing common format event; and

applying one or more rules from a set of rules to the knowledge-containing common format event to generate the alert indication.

2. (Original) The method of claim 1, wherein the common format event contains at least a generic description of a specific event occurring as part of each device output.

3. (Original) The method of claim 1, wherein generating the knowledge-containing common format event further comprises comparing the common format event for each network device to a number of knowledge base table entries contained in a knowledge base table, wherein knowledge is added from one or more of the

knowledge base table entries when a match between the translated common format event and the entry in the knowledge base table is made.

4. (Original) The method of claim 1, wherein the enterprise devices are selected from the group consisting of a server, a firewall, a modem, a work station, a router, a remote machine, an intrusion detection system, an identification and authentication server, network monitoring and management systems, network components, and one or more combinations thereof.

5. (Previously presented) The method of claim 1, wherein the translating step further comprises:

matching data values in the device output with a signature specification for each enterprise device, the signature specification containing:

- a number of signatures;
- a first location identifier for each signature; and
- a first key;

wherein the signature is a listing of names found in the device output, the first location identifier determines the method used to locate the name in the device output, and the first key determines where to locate the name in the device output;

identifying a message type from a plurality of message types for each enterprise device based on the device output as part of the translated common format event;

producing the remainder of the translated common format event in argument name and argument value pairs using an argument specification, the argument specification containing;

a listing of arguments;

a field type;

a second location identifier for each argument; and

a second key;

wherein each argument is a listing of argument names for inclusion in the translated common format event, the field type specifies the form of an argument value found in the device output, the second location identifier determines the location of each argument value, and the second key locates the argument value in the device output to be displayed with the argument name.

6. (Original) The method of claim 1, wherein the knowledge-containing common format event comprises one or more names selected from the group of a device alert, a generic alert, a threat severity, a benign explanation, a recommended action, a common vulnerabilities and exposure code, a conclusion, and a category code, and a corresponding value for each name.

7. (Original) The method of claim 1, wherein one or more rules determine when or whether the knowledge-containing common format event is generated, and final rule-based additions content of such generated events.

8. (Original) The method of claim 7, wherein the rule requires that the each output occur a number of times over a period of time before an alert indication is generated.

9. (Original) The method of claim 1, wherein the output is one of an unauthorized login, an unauthorized physical entry, and an attempt to bypass a firewall.

10. (Previously presented) The method of claim 3, wherein the translating step further comprises:

matching data values in the device output with a signature specification for each enterprise device, the signature specification containing:

- a number of signatures;
- a first location identifier for each signature; and
- a first key;

wherein the signature is a listing of names found in the device output, the first location identifier determines the method used to locate the name in the device output, and the first key determines where to locate the name in the device output;

identifying a message type from a plurality of message types for each enterprise device based on the device output as part of the translated common format event;

producing the remainder of the translated common format event in argument name and argument value pairs using an argument specification, the argument specification containing;

- a listing of arguments;
- a field type;
- a second location identifier; and
- a second key;

wherein each argument is a listing of argument names for inclusion in the translated common format event; the field type specifies the form of an argument value found in the device output, the second location identifier determines the location of each argument value, and the second key locates the argument value in the device output to be displayed with the argument name.

11. (Original) The method of claim 10, wherein the rule determines when or whether the knowledge-containing common format event is generated.

12. (Original) The method of claim 11, wherein the rule requires that each output occur a number of times over a period of time before an alert indication is generated.

13. (Original) The method of claim 1, wherein the alert indication includes at least a text message describing the event contained in the output of the enterprise device.

14. (Original) The method of claim 13, wherein a threat level is included as part of the alert indication.

15. (Original) A system for producing at least one alert indication based on a number of events derived from an enterprise comprising:

a plurality of enterprise devices, each device capable of producing an output;

a number of translation files, the translation files allowing the output to be translated into a common format event;

a number of knowledge base table files, matching of the common format event with one or more of the knowledge base table files adding knowledge from the matched file to generate a knowledge-containing common format event;

a number of rule files, the rule files governing generation of the alert indication.

16. (Original) The system of claim 15, wherein the enterprise devices are selected from the group consisting of a server, a firewall, a modem, a work station, a router, a remote machine, an intrusion detection system, an identification and

authentication server, network monitoring and management systems, network components, and one or more combinations thereof, or any generator of data streams on the computer network.

17. (Original) The system of claim 15, wherein the knowledge-containing common format event comprises one or more names selected from the group of a device alert, a generic alert, a threat severity, a benign explanation, a recommended action, a CVE, a conclusion, and a category code, and a corresponding value for each name.

18. (Original) The system of claim 15, wherein the common format event comprises a message, and a number of name and value pairs derived from the output of the enterprise device.

19. (Original) The system of claim 17, wherein the rule files govern at least the frequency of the generation of the alert indication.

20. (Original) The system of claim 19, wherein the common format event comprises a message, and a number of name and value pairs derived from the output of the enterprise device.

21. (Original) The method of claim 7, wherein the rule adds information to the knowledge-containing common format event.

22. (Previously presented) The method of claim 11, wherein the rule adds information to the knowledge-containing common format event.

Evidence appendix

None

Related proceedings appendix

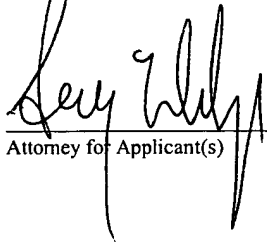
None

Conclusion

If there are any questions relating to the above, please telephone the undersigned Attorney for Applicant.

CERTIFICATE OF MAILING

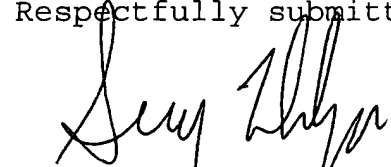
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 31, 2006.



Attorney for Applicant(s)

May 31, 2006
Date of Signature

Respectfully submitted,



Serge J. Hodgson
Attorney for Applicant(s)
Reg. No. 40,017
Tel.: (831) 655-0880



GUNNISON, MCKAY & HODGSON, L.L.P.

GARDEN WEST OFFICE PLAZA, SUITE 220

1900 GARDEN ROAD

MONTEREY, CALIFORNIA 93940

(831) 655-0880

FACSIMILE (831) 655-0888

May 31, 2006

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

RE: Applicant(s): John B. Beavers

Assignee: Symantec Corporation

Title: SYSTEM AND METHOD FOR TRACKING AND FILTERING
ALERTS IN AN ENTERPRISE AND GENERATING ALERT
INDICATIONS FOR ANALYSIS

Serial No.: 10/080,574 Filed: February 25, 2002

Examiner: Nirav B. Patel Group Art
Unit: 2135

Docket No.: SYMC1023

Dear Sir:

Transmitted herewith are the following documents in support of the Notice of Appeal filed on April 21, 2006 in the above application:

1. Return receipt postcard;
2. Check in the amount of \$500.00 for filing a brief in support of an appeal;
3. This Transmittal Letter (2 pages); and
4. Appellant's Brief (25 pages).

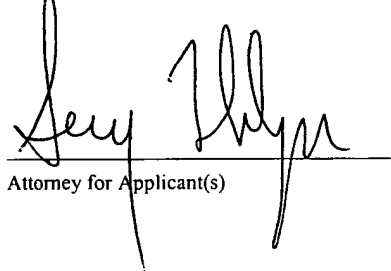
Transmittal Letter
Serial No. 10/080,574
May 31, 2006

☒ Conditional Petition for Extension of Time: If an extension of time is required for timely filing of the enclosed documents after all papers filed with this transmittal have been considered, Applicant(s) hereby petition for such an extension of time.

☒ The Commissioner is hereby authorized to charge any additional fees required for consideration of the enclosed documents, and to credit any overpayment of fees to Deposit Account No. 50-0553.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 31, 2006.




Attorney for Applicant(s)

May 31, 2006

Date of Signature

Respectfully submitted,



Serge J. Hodgson
Attorney for Applicant(s)
Reg. No. 40,017